Microsoft

Exchange 2000 Migration:

Deploying the Active Directory Connector within Microsoft

White Paper

Microsoft® iT Showcase

Best practices, experiences and global solutions from Microsoft IT

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

CONTENTS

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Outlook, Windows and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

EXECUTIVE SUMMARY.....1

INTRODUCTION.....5

ITG ENVIRONMENT.....7
- **Organizational Structure** **7**
- **Network Structure** **7**
- **Forest Structure** **8**
- **Active Directory Performance Testing** **9**
- **Messaging Structure** **10**
- **Administrative Structure** **13**

EXCHANGE 2000 ADC ARCHITECTURE.....15

ADC DEPLOYMENT.....18
- **Team Structure** **18**
- **Team Goals** **19**
- **Timeline** **20**
- **Planning Considerations** **21**
- **Deployment Phases/Checkpoints** **23**

LESSONS LEARNED.....34

FOR FURTHER INFORMATION.....36

EXECUTIVE SUMMARY

Managing Microsoft's complex messaging environment is a team effort, requiring tremendous inter-group cooperation, planning, and flexibility. Message traffic averages about 7.5 million messages a day, with 800,000 messages a day to and from the Internet. As of this writing Microsoft's Information Technology Group (ITG) has begun the process of migrating its internal messaging infrastructure from Microsoft® Exchange Server 5.5 to Exchange 2000. A key business requirement during the migration period is preserving the rich data currently housed in the Exchange 5.5 directory service. In any large environment, the migration will take some time, and during the transition the Exchange Server 5.5 directory and Microsoft Windows® 2000 Active Directory™ service must be kept synchronized. A temporary but critically important step in that migration is deployment of the Exchange 2000 Active Directory Connector (ADC).

Directory services function like the white pages of a telephone book. Using specific input (for example, a person's name), a user can receive specific output (a person's address and telephone number). Directory services also provide the functionality of yellow pages. Using general input (e.g., "where are the printers?"), a user can receive a listing of printer resources nearest to them. Microsoft employees rely on this kind of information in the Exchange 5.5 directory every day, to find out another employee's phone number, office location, or distribution list membership, for example. With the deployment of Windows 2000, Active Directory provides all this information and more.

Since even before its first release in 1996, ITG has used the Exchange 5.5 directory service internally at Microsoft to provide the corporate messaging environment with:

- **Multimaster replication,** for built-in redundancy.
- **Remote Procedure Call (RPC)–based replication** within a site, **and mail-based replication** between sites, to ensure that all directory updates are quickly and efficiently propagated to all other Exchange servers in the organization.
- **Scalability and a transaction-based database.** Exchange Server 5.5 is scalable to hundreds of thousands of users. The transaction-based database ensures data integrity in the event of a problem, providing a record of recent changes that can be replayed after backup restoration.

With the advent of Active Directory, the directory database provided by the network operating system is now capable of holding all user account details, security and messaging information. This means that a separate directory for Exchange 2000 is no longer necessary. Exchange 2000 is fully integrated with Active Directory and does not include its own directory service (DS).

Integration of the two directory services provides users with access to user and configuration information, object browsing, security, and name resolution. The Active Directory Connector is the Exchange 2000 component

responsible for synchronizing Active Directory with the Exchange Server 5.5 DS during the migration period.

Exchange 2000 has been designed to simplify integration and migration to the Active Directory service while providing full backward compatibility. Integration of the two directory services offers ITG many benefits, including:

- **Improved replication**. In the Exchange 5.5 environment, Exchange server objects could only be modified in the specific site in which the object was created. In contrast, the Active Directory service allows any object to be modified on any server that contains a full replica of the site, dramatically increasing replication flexibility. When directory objects were changed in Exchange Server 5.5, the entire object had to be re-replicated throughout the organization, because Exchange 5.5 supported only object-level replication. Active Directory employs a per-property replication (only the changed property is replicated instead of the entire object), reducing replication time and replication conflict because different attributes of the same object can now be modified in two locations at the same time.
- **Unified administration**. In a mixed Exchange 5.5 and Exchange 2000 messaging environment, synchronized directory objects can be managed from either Active Directory, through the Users and Computers Microsoft Management Console (MMC) snap-in, or from the Exchange directory (through the Exchange MMC snap-in), and the changes can then be replicated to the "legacy" Exchange servers depending on the synchronization direction of the ADC connection agreement. During the migration period ITG still uses the Exchange 5.5 administration tool for some administrative tasks in the Exchange 5.5 directory.
- **Extensible schema.** By default, Active Directory contains over 120 classes and 800 attributes. However, because the schema is extensible, Exchange 2000 installation can add another 155 classes (for example, Connector) and 818 attributes (for example, Message-Quota). In addition, 270 attributes are marked for replication to the global catalog for global retrieval. This allows ITG to preserve the rich data already housed in the Exchange 5.5 DS, merging it into Active Directory.[1]
- **Client access protocols.** Internet clients interact directly with Active Directory for recipient lookups using the Lightweight Directory Access Protocol (LDAP). Existing Exchange 4.0 and 5/5.5 clients interact with Active Directory using the existing Messaging Application Programming Interface (MAPI) RPC protocol, so no desktop changes are required in the upgrade. The net effect for ITG users is a transparent upgrade.
- **Single common programming interface.** LDAP, Collaboration Data Object (CDO) and/or Active Directory Services Interface (ADSI) scripts can be written based on one directory instead of two. This speeds ITG application development and facilitates reuse in the future. For example, the CDO System Management interface provides “mailbox-enable” and

[1] Schema adds/changes are listed in the .ldf files in the Exchange 2000 setup directory.

"mail-enable" methods, which allow ITG to automate DS changes.

Bringing the two directories (Active Directory and Exchange 5.5 directory) together has enterprise-wide impacts, affecting many different ITG areas of responsibility. Both Windows 2000 and Exchange administrators must cooperate and coordinate their formerly separate administrative responsibilities to an unprecedented degree for successful Active Directory Connector and Exchange 2000 deployment. In addition to natively supporting Windows security authority, there are three main areas where Exchange 2000 Server heavily relies upon Windows 2000: directory, transport, and name resolution.

- **Directory.** Unlike previous versions of Exchange, Exchange 2000 does not include its own directory service. Instead it relies upon Active Directory in Windows 2000 to provide functionality such as the Global Address List, Address Book Views, and Offline Address Books. In the Exchange 2000 environment ITG has only to manage one DS (Active Directory), instead of three (Exchange 5.5 DS, Active Directory, and Windows NT® SAM).
- **Transport.** Base Internet protocol stacks, such as Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP) are configured as part of the Windows 2000 operating system. The operating system and other components make use of these stacks. For example, it is possible to replicate Active Directory information using SMTP rather than RPC. Exchange 2000 installation extends these stacks with additional command verbs and advanced routing components to provide all of the functionality required for an enterprise-class messaging and collaboration system. These extensions are installed as a set of *Sinks* that are registered with each protocol.
- **Name Resolution.** Exchange 2000 is a network-oriented product relying on underlying network infrastructure and protocols to carry data. Clients communicate with servers to access collaboration data, and servers communicate with other servers to route messages. In Windows NT Server 4.0, the Windows Internet Name Service (WINS) provided NetBIOS name resolution and Domain Name System (DNS) was used for winsock-based name resolution. By default, previous versions of Outlook and Exchange clients use the winsock layer for communications and consequently DNS as the preferred name resolution technique. In Windows 2000, other components, such as logon and domain validation, have moved over to DNS as the primary name resolution method.

In February 2000, ITG deployed the Exchange version of the ADC within the corporate data center in Redmond, Washington. The ADC populated Windows 2000 Active Directory with the directory information then existing in the corporate Exchange 5.5 DS.

This paper describes the deployment activities associated with this temporary but critical step in the migration of the Microsoft enterprise network's messaging infrastructure from Exchange 5.5 to Exchange 2000.

The infrastructure elements detailed in this paper include the Exchange

INTRODUCTION

2000 Active Directory Connector, Windows 2000 Active Directory namespace (DNS, forests, domains, sites), administrative structure and server specifications. Note that the domain names provided are for illustration only and do not necessarily reflect actual names used for security reasons.

Microsoft's global network infrastructure comprises both an inward-facing network (known as corpnet) and a customer-facing network (Internet properties). This paper focuses primarily on the corpnet messaging migration. This document is based on initial design efforts begun by ITG before the release of Windows 2000 and Exchange 2000. It is important to note ADC planning and deployment has undergone frequent change and will continue to be refined.

This paper is intended for Exchange and Windows operations and engineering staff, IT architects, and consultants at the enterprise level. It is not intended to serve as a procedural guide. Each enterprise environment is comprised of unique circumstances and, therefore, each organization should adapt the plans and "lessons learned" described in this paper to meet their specific needs.

A temporary but crucial step in enterprise migration to Exchange 2000 is the consolidation by the Exchange 2000 ADC of two separate entities, the Exchange 5.5 mailbox and its associated Windows user account, into one entity – a Windows 2000 mailbox-enabled user.

The Windows 2000 Active Directory must be fully populated with user objects for all Exchange 5.5 mailboxes (with appropriate Exchange attributes filled out) before the first Exchange 2000 server deploys, through upgrade or addition, in the organization. The Exchange 2000 server will have no direct access to the Exchange 5.5 directory – the Windows 2000 Active Directory is the Exchange 2000 server's directory. Consequently the Active Directory service must accurately reflect the information in the Exchange 5.5 directory, and the two directories must be kept synchronized during the migration period.

The Exchange 2000 ADC creates and maintains this bond between an Exchange 5.5 mailbox and a Windows user until the last Exchange 5.5 server in the organization has been upgraded or decommissioned. Once the organization is "pure Exchange 2000" (native mode) the ADC is no longer needed. An Exchange 2000 organization is said to be in "native" mode when Exchange 5.5 servers no longer exist in the organization.

The ADC synchronizes changes in one or both directions, depending on how it is configured, which depends partly an organization's administrative model, and how Windows 2000 users are initially created. The ADC synchronizes two distinct types of directory objects present in the Exchange 5.5 directory:

- **Recipients** (Mailboxes, Distribution Lists, Custom Recipients)
- **Configuration** information (Connectors, Monitors, Protocols)

The Exchange 5.5 recipient objects become one of the following native Windows 2000 objects in the Active Directory domain container:

- **Mailbox:** an Exchange 5.5 mailbox becomes a Windows 2000 user who has been "mailbox-enabled"; in other words, a user with an e-mail address, information that indicates the Exchange server to which the user's mail should be routed, and to which the user connects to receive mail. Mailbox-enabled users are security principals (with logon rights) in Active Directory that can send and receive messages. Implicitly, these user types also have SMTP addresses.
- **Distribution Lists:** Windows 2000 uses groups to reduce the number of objects that require direct administration. Users are placed into groups, which are further consolidated into other groups, allowing bulk administration. Exchange 2000 Server uses this concept of bulk administration and permission granting, but it also uses groups as distribution lists to which messages can be sent. Active Directory supports two types of group, Security and Distribution, and each of these can be mail-enabled, and scoped to Domain Local, Global, and Universal. ITG uses security groups for granting privileges and rights for administration to certain configuration and server objects, such as Public folders.
- **Custom Recipients:** In general, an Exchange 5.5 Custom Recipient is represented as a mail-enabled Contact in Active Directory; that is, a Contact with an e-mail address and (optionally) information that allows Exchange to properly route the mail. All mail-enabled contacts can have an SMTP address.

With Exchange 2000 integration into Active Directory, any object in Active Directory can be mail-enabled. To mail-enable a native Windows 2000 objectClass or third-party objectClass, the schema definition of the object can be modified to include the Exchange-Recipient Auxiliary class and set the LDAP mail attribute on the object. This modification allows Exchange 2000 to route mail addressed to this object. For example, the Windows 2000 Server object could be mail-enabled and the **target-address** attribute could be set to *server_admin@ms.com*. Messages can then be sent directly to the server, for example to request additional disk space, and the messages would be routed to the server administrator’s mailbox.

Replicating configuration information involves an important change in the way sites are handled. The site concept in the Exchange 5.5 directory defined the unit of administration, namespace, and dictated message routing. In contrast, an Active Directory site does not include a unit of namespace. For example, multiple sites may exist within a single domain, or a single site may span multiple domains. In Windows 2000, a site is a local, logical collection of Internet Protocol (IP) subnets that share high-speed connectivity (Local Area Network speeds) with one another. Synchronous RPC is used for replication of the domain-naming context within a domain.

Table 1 details some of the differences between Exchange 2000/Windows 2000 and Exchange 5.5 “sites” that are important for enterprise Windows

and messaging staff to understand.

Exchange 5.5 Site	Active Directory Site
Unit of namespace in the X.500 structure	No relationship with Active Directory domain structure; namespaces can be separated from domain structure
Unit of administration	No relationship to Active Directory administration; administrative structure can be constructed according to organizational needs
High-bandwidth, reliable network connections between all servers	High-bandwidth, reliable network connections between all servers
Defines single-hop message routing	Has no effect on message routing and little affect on the rest of Exchange 2000 Server

Table 1: Differences in the term "Site"

Organizational Structure

As of this writing, ITG comprises roughly 2,500 people worldwide, including full-time employees, contractors and interns, who are responsible for managing roughly 50,000 users, 100,000 desktops, and thousands of servers that span 450 sites in 62 countries.

The primary business of Microsoft is software design. Consequently, ITG has business drivers that are unique among global enterprises. For example, in addition to running the enterprise IT utility, ITG plays a strategic role as one of Microsoft's early adopters, testing and deploying Microsoft software before customer release, a process known internally as "eating our own dogfood".

Like other global enterprises, ITG is organized into functional groups, including those that run the IT utility, as well as those responsible for HR, finance, legal, and other business processes. The main IT groups involved in the ITG Exchange 2000 deployment include:

- **Global Networking and Systems** (GNS) provides corporate computing and communication infrastructure services. GNS is responsible for designing, implementing, and supporting IT solutions to meet enterprise requirements of Microsoft's data communications around the globe. This includes Microsoft's corporate Intranet (corpnet) and Internet presence. For example, GNS personnel determine the sizing and placement of Windows 2000 domain controllers (DC), global catalogs (GC), and Exchange 2000 servers.

- **IT Security (ITSEC)** comprises several groups providing both physical and information security services. The Domain Security Management group, for example, is responsible for the creation and management of domains, Windows permissions, and disk management support.
- **Operations IT (OPSIT)** manages the corporate data centers and works with Microsoft business units in applications design, development and support.
- **End User Services/Application Platform Services (EUS/APS)** manages user accounts and messaging operations, corporate desktops, and the global helpdesk. Enterprise Applications and Services (EAS) manages enterprise data services, such as HR applications and finance.

In addition, the deployment team for Exchange 2000 includes members from other areas, such as the Windows 2000 and Exchange 2000 product development groups and Product Support Services (PSS). Because ITG usually deploys so early in the product cycle that product documentation is not yet complete, User Documentation groups were also involved as observers in various stages of the deployment.

Network Structure

ITG undertook a global network infrastructure upgrade roughly simultaneously with the production deployment of the Windows 2000 network operating system and Exchange 2000. Maximum network throughput under the old design was limited by the gigaswitch serving as the corporate hub (3.2 gigabits/sec). To break this bottleneck, and to accommodate future growth, a very high-speed (170 gigabits/sec) Asynchronous Transfer Mode (ATM) backbone was installed.

This significantly increased available bandwidth for all network applications, such as Exchange 2000. Increased bandwidth between physical locations gave ITG the opportunity to revisit the Exchange 5.5 Server network architecture. For example, because of improved replication, more Public Folder servers might be hosted in remote sites.

The corpnet internal network physical topology is comprised of:

- More than 200 Wide Area Network (WAN) circuits
- Over 1,000 routers
- More than 140 ATM switches
- Over 900 Local Area Network (LAN) switches (100 Mbps to servers, 10 Mbps to desktops)
- In excess of 2,500 IP Subnets
- More than 100,000 LAN ports

Forest Structure

The corpnet.ms.com Windows 2000 forest is the primary container of ITG-controlled corporate domain user accounts, groups and corporate resources. The root of the forest is the corpnet.ms.com domain. This domain is a top-level placeholder that contains a limited number of corporate-wide resources and administrative accounts only.

Domains within the corpnet.ms.com forest have multiple external trusts to child domains in the product development forests, as shown in Figure 1. Multiple forests in this design isolate the production environment from Active Directory schema changes that are necessary in the product development environments, yet allow ITG to centrally manage development forest users and groups and other network resources.

The prefix (DC=corpnet) is added to ms.com in order to differentiate the corpnet from the Internet namespace.

Figure 1 shows a high-level view of the Microsoft enterprise Windows 2000-based forest structure.

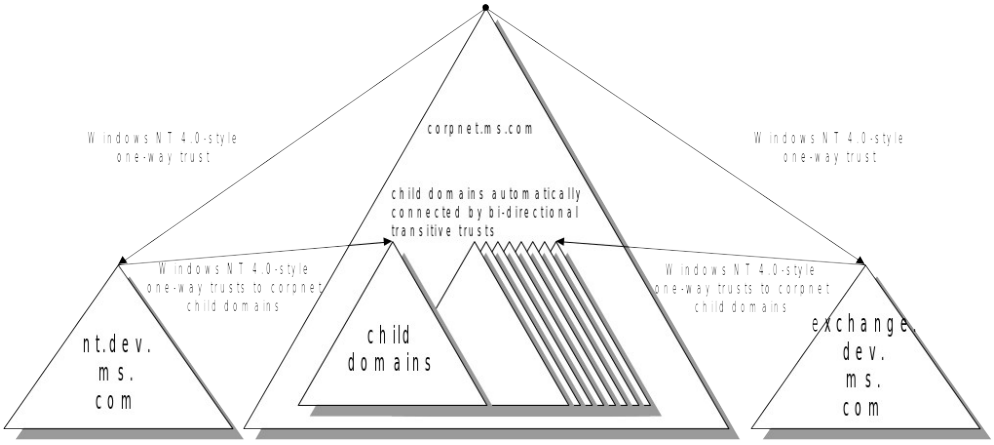
corpnet.ms.com
Windows NT 4.0-style one-way trust
Windows NT 4.0-style one-way trust
child domains automatically connected by bi-directional transitive trusts
Windows NT 4.0-style one-way trusts to corpnet child domains
Windows NT 4.0-style one-way trusts to corpnet child domains
nt.dev.ms.com
child domains
exchange.dev.ms.com

Figure 1: High-level Forest Structure

Active Directory Performance Testing

ITG designed its Windows 2000 Active Directory topology with Exchange 2000 needs in mind, and conducted early tests on the functions users most often exercise to forecast their effects on Active Directory, and therefore on DC/GC replication traffic. For example, Exchange clients display directory information obtained from GC servers. Attributes Microsoft employees formerly obtained in the Exchange 5.5 DS (such as CostCenter) are flagged for GC replication, because during the transition period, clients from both environments need access to this data in Active Directory.

ITG tested many factors affecting replication traffic including:

- **Global Address List** - Microsoft users see Microsoft Outlook® not just as a messaging client but also as a means to access phone numbers, addresses, and other organizational information, such as manager name and department. GCs support the MAPI protocol as well as LDAP, so no change to clients running Outlook was required.
- **Internally developed line of business applications** relying on custom CDO and/or ADSI queries for directory data. For example, a workflow application that requires access to an Exchange 5.5 Custom Attribute holding a manager's budgetary limit.
- **Address Book Lookups** for sending and routing messages.

ITG's preliminary testing showed each additional attribute tagged for GC replication incurred roughly an additional 100 bytes of replication data per object. Testing predicted that Windows 2000/Exchange 2000 replication traffic would be far less than that of the existing Exchange 5.5 topology because:

- Each Exchange 5.5 server in the organization held a full copy of the Exchange directory, whereas Active Directory only replicates to DC/GC servers.
- Changes to an Exchange 5.5 object caused the entire object to replicate

to the rest of the Exchange organization, at roughly 5 kilobytes (KB) intra-site and 1 KB inter-site. Active Directory replication is per-property replication (only the changed property is replicated), so the replication payload is much smaller.

- Both the Exchange 5.5 directory and Windows NT 4.0 DCs replicated around the company network. Active Directory consolidates these two directories into one.
- Exchange 5.5 Distribution Lists are replaced with mail-enabled groups in Active Directory. Universal groups and their membership are replicated in the GC. Global group names are also replicated, but not group membership

Based on preliminary testing results, the existing Exchange 5.5 infrastructure, and the concurrent infrastructure upgrade process (which consolidated DCs and GCs into "DC/GC" servers) ITG developed the following guidelines for corpnet DC/GC placement:

- At least one DC/GC per site of 1,000 users or more. For larger sites (more than 1,000 users), additional DC/GCs will be placed according to the needs determined for acceptable user response time.
- A DC/GC in each existing Regional Data Center (RDC) or Site Data Room (SDR) where there is at least one Exchange 5.5 server.
- At least one DC/GC in the Redmond Datacenter for each production domain so that centralized administrative changes can be mastered locally and the changes replicated automatically by multi-master replication.

Messaging Structure

Hardware Profile

As of this writing ITG maintains roughly 200 Microsoft Exchange 5.5 servers worldwide in almost 100 cities, with roughly forty percent of these located at the corporate campus in Redmond, Washington. Exchange servers are typically deployed as dedicated-service servers, with similar hardware specifications, but differing messaging roles, as shown in Table 2.

Server Type	Count
Mailboxes	133
PFS[2]	16
HUB	23
IMC[3]	20
Fax	5
Free/Busy	5
Key Mgmt	1

Table 2: Server Distribution

These Exchange servers are grouped into 13 Exchange sites, with 30 site

[2] Public Folder Server
[3] Internet Mail Connector

connectors, comprising one Exchange organization that generates more than 500,000 Exchange application events per day.

Message traffic averages about 7.5 million messages a day with 800,000 messages a day to and from the Internet. Microsoft's pre-Exchange 2000 production environment contains about 50,000 mailboxes (average size=27 Mb), more than 35,000 Distribution Lists, and 90,000 Public Folders worldwide, running exclusively on Exchange Server 5.5, Service Pack 3.

ITG's Exchange 5.5 mailbox servers were built and managed based on the limitations imposed by the time ITG requires to securely backup and restore each Exchange database. Since Exchange 5.5 was limited to one database for private mail, and one database for shared folders, the practical limitations of database restore times limit each ITG Exchange 5.5 messaging server to roughly 1,000 mailboxes. Each Exchange 5.5 mailbox is limited to 50 MB [4].

In contrast, Exchange 2000 supports multiple storage groups on a single server, each holding up to 6 databases, allowing ITG to host many more users per server, increase mailbox limits, and still maintain goals for backup and restore times, which is the key server-sizing criteria. Increasing user density per server allows ITG to implement much larger servers (for example 3,000 users at 100 Mb per mailbox) and thereby reduce the total number of servers in the environment. Maintenance and restore times are also reduced, because multiple databases can be serviced in parallel without affecting all users on the server.

Representative high-level hardware specifications for different sizes of Exchange server are detailed in Table 3. Note that circular logging is disabled for all standard Exchange mailbox servers and information store database files. Transaction log files are placed on separate disk arrays as a standard operating procedure. This requirement affects the storage requirements for each size server.

Circular logging, if enabled, causes the log files to be wrapped as needed based on server activity, preventing continuous build up of the Exchange database transaction log files on the hard drive. However, the disadvantage is that differential and incremental backups cannot be performed while circular logging is enabled because they rely on the .EDB file and all past transaction logs to create a current database. If all past transactions are not available, the recreation is not possible. Instead, ITG disables circular logging and performs daily backups.

[4] Based on an operational requirement of no more than 3 hours daily at 40gb/hr for online backups.

Small Mailbox Server. Supporting up to 500 mailboxes.		
CPU	**RAM**	**Hard drive**
1@ 200 MHz or faster	256 Mb	25 Gb RAID array, redundant controllers
Medium Mailbox Server. Supporting up to 1,000 mailboxes		
CPU	**RAM**	**Hard drive**
4@200 MHz or faster	512 Mb	125 Gb RAID array, redundant controllers
Large Mailbox Server. Supporting up to 3,000 mailboxes		
CPU	**RAM**	**Hard drive**
8@550 MHz or faster	4Gb	600 Gb RAID array, redundant controllers Cluster Technology
Public Folder Server		
CPU	**RAM**	**Hard drive**
2@200 MHz or faster	512 Mb	50 Gb RAID array, redundant controllers

Table 3: Server Roles and Specifications

Software Profile

Because Exchange 2000 supports all clients that work with Exchange Server 5.5, and the majority of Microsoft employees use Windows 2000 Professional and the Outlook 2000 messaging and collaboration client, no client issues were anticipated. Once the Exchange 2000 production server is in place, Exchange clients accessing the Exchange 2000 server access the directory held on the nearest GC server over MAPI. Microsoft Outlook 2000 clients access the GC directly. Earlier versions of Outlook (earlier than version 8.5.6204.0) are referred to a GC by an Exchange 2000 proxy service (DSProxy).

User Profile

ITG characterized a generic corporate Exchange user profile for testing, including the activities that generate roughly ninety percent of messaging traffic. To simulate “real world usage” each test run was randomized in a reproducible way so that load was consistent, but usage patterns differed.

The profile’s primary tasks include reading, browsing, moving, deleting and sending. A similar sample profile is detailed in Table 4.

Characteristic	Value
Private Store Size Limit	100 Mb
Average Number of Logon/LogOff's Per Day	6
Average Server Store Usage	32 Mb
Days to Retain Deleted Item	7
Average Message Size (sent)	27 Kb
Average Number of Messages Sent Per Day (each to 20 recipients)	50
Average Number of Public Folder Accesses Per Day	20
Average Number of Calendar Accesses Per Day (excluding auto-syncing, etc)	25
Average Number of Messages Received Per Day	200
Of the 200 new messages: DELETE 30 MOVE 30 COPY 30 REPLY TO 30 REPLY TO ALL 20 FORWARD 10 (to 40 new recipients) Of the 200 new messages - 10 are CALENDAR invitations	

Table 4: Sample User Profile

Administrative Structure

Server Administration

In the Exchange 5.5 environment, ITG messaging and Windows NT 4.0 server administrators separately managed responsibilities by placing Exchange servers in a trusted Windows NT 4.0 resource domain. In the Windows 2000/Exchange 2000 environment resource domains are replaced by Windows 2000 organizational units (OUs). Exchange 2000 servers are placed into ous and administration on those ous is delegated to messaging administrators.

In the Exchange 5.5 environment, ITG grouped Exchange servers into sites not only for administration, but also for directory replication and message routing. Exchange administrators had to configure explicit message routing and directory replication connections between sites. ITG designed its Exchange 5.5 implementation to minimize conflict between the need for large sites (for administration purposes) and network bandwidth limitations imposed on those sites by the site level message routing and directory replication algorithms.

In the Windows 2000/Exchange 2000 environment, sites have a different fundamental definition and purpose:

- **Administration** is managed by grouping Exchange 2000 servers into administration groups (AGs).
- **Directory replication** is handled at the network operating system level independent of Exchange 2000. In Windows 2000, a site is defined as a

collection of IP subnets connected by high bandwidth, so RPC replication is automatically handled by Windows 2000.

- **Message routing** is organized by grouping servers into routing groups (RGs) to control message flow. In Exchange 2000 routing groups and administration groups need not be the same. ITG can place Exchange 2000 servers into administration groups to match their operational structure, divide servers into routing groups to match the WAN topology, and leave directory management to the Windows 2000 team.

When in native mode (“pure” Exchange 2000), Exchange 2000 Server provides the ability to separate administrative and routing activities (Exchange 2000 administration groups and routing groups) in the same way as the Windows 2000 namespace provides delegation of administration with little regard to the underlying network structure, which is accounted for in site topology. Note that during the migration, while coexisting with Exchange 5.5, administration groups and routing groups are the same and display as sites when viewed in the Exchange 5.5 directory. ITG will be able to redefine routing groups once every server in the administration group is upgraded to Exchange 2000.

The ADC, Site Replication Service (SRS) and Recipient Update Service (RUS) are new services (detailed in the next section of this paper), and are administered by the deployment team. Changes in operational practices and server administration models arising from new administrative flexibility and services, such as Unified Messaging and Exchange Conferencing Services, are under review during the migration.

User Administration

In the Exchange 5.5 environment, one ITG group (MessageOps) was responsible for managing Exchange recipient objects, while another group (Accounts) was responsible for Windows user accounts. In the Exchange 2000 environment, parameters such as mailbox location and size limits are just additional attributes on user objects in Active Directory, and can be managed by either group (with appropriate permissions). During the migration both ITG groups, as well as other stakeholders such as the security group, are examining new user administration models made possible by DS unification. For example, it is possible to “master” Exchange mailbox changes in Active Directory, and to delegate authority for mailbox administration at a fine-grained level.

The Exchange 2000 ADC is fundamentally a replication and attribute mapping engine - taking information from one LDAP directory (Exchange 5.5) and replicating it to another LDAP directory (Active Directory). Functions of the ADC include:

- Leveraging the standard replication mechanism of querying for deltas based on the last known Update Sequence Number (USN).
- Running on a scheduled or continual basis.

- Merging objects with similar semantics.
- Converting Exchange 5.5 Mailboxes to Windows 2000 Mailbox-enabled users.
- Converting Exchange 5.5 Custom recipients to Windows 2000 Contacts (mail-disabled by default).
- Converting Exchange 5.5 Distribution lists to Windows 2000 Universal Distribution Groups (UDG).
- Replicating Exchange 5.5 site configuration information to Windows 2000 Administration and Routing groups.

Deploying the ADC is the first step in the process of unifying information in the two directories and consolidating two separate entities (Exchange 5.5 mailbox and Windows 2000 user) into one – a Windows 2000 mailbox-enabled user. Figure 2 shows a high-level view of the function of the ADC.

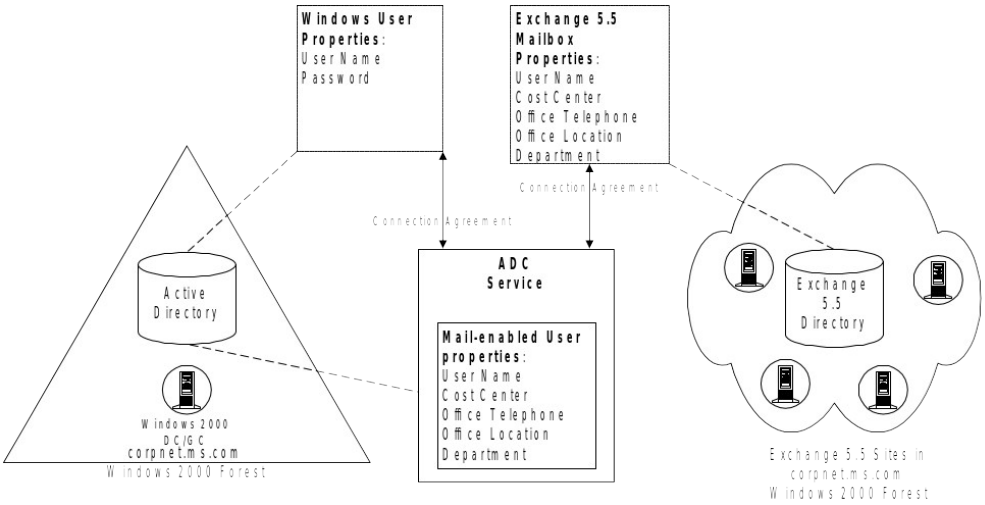

Figure 2: Exchange 2000 ADC Function

Note that there are two implementations of the ADC, one (shipped with Windows 2000) for connecting Active Directory and the Exchange 5.5 directory (when no Exchange 2000 Server is present), and one for connecting Exchange 5.5 and Exchange 2000 (which uses Active Directory). The Windows 2000 ADC is a subset of the Exchange 2000 ADC, and allows only *directory* replication of objects in the site-naming context (such as mailboxes, custom recipients, and distribution lists) between Exchange 5.5 and Active Directory.

The Exchange 2000 ADC version adds the ability to exchange *configuration* information between the Exchange 5.5 organization and Active Directory. Regardless of the connection agreements (CAs) created for the Windows 2000 ADC (if present), the Exchange 2000 ADC also creates a read-only Configuration CA that performs this bi-directional configuration information transfer (configuration of the CA itself is read-only, the ADC writes changes to the appropriate directories). Configuration CAs are created automatically, as opposed to “user” CAs that are installed, configured and controlled by the

administrator. Since the Exchange 2000 ADC version is a superset of the Windows 2000 version, if the Windows 2000 version was not already installed, it is installed with the Exchange 2000 ADC.

The Exchange 2000 ADC comprises two additional components, which can be run on a dedicated Windows 2000 member-server or on top of Exchange 2000:

- The ADC service, which can be started and stopped just like any other service.
- The ADC MMC snap-in, which is used to configure the replication relationships between the two directories (CAs).

The CA is like the work order to the replication engine, defining replication characteristics such as the server names to contact for synchronization, object classes to synchronize, target containers, and synchronization schedule. A single ADC can host multiple CAs –each connecting Active Directory to a single Exchange Server site, or to multiple Exchange Server sites (one per CA). ITG hosts all necessary CAs on one dedicated ADC Windows 2000 member server.

Specifically, a connection agreement defines the following:

- Directory(s) to be synchronized.
- Windows 2000 Server synchronization objects.
- Exchange Server 5.5 synchronization objects.
- The direction in which synchronization takes place, either “one-way” or “two-way”.
- Synchronization schedule, which directly affects server processing load. It is important that computers running the ADC are appropriately specified (CPU and memory) and well-connected (LAN speed). The default synchronization schedule is 8 hours, but may be adjusted for each CA in the case of multiple CAs to one Exchange 5.5 site for more granular container control. For example, ITG can set one CA schedule to once per week, and another to once per day. For the initial ADC synchronization ITG scheduled the CA’s apart from each other because of the amount of data that would be passing through the connection agreements.
- Method for deleting objects.
- Advanced options, including:
    - Attribute mapping.
    - New object creation.
    - Authenticating Directories.
    - Specifying which ous or containers to synchronize.

Configuring the synchronization direction of the CAs is based on administrative strategy. For example, since current ITG mailbox

administration is from the Exchange 5.5 DS, the CA is configured “one-way”, synchronizing from Exchange 5.5 to Active Directory.

Two new services, important to ADC function, are installed by Exchange 2000 server setup: the Site Replication Service (SRS) and Recipient Update Service (RUS).

The Exchange 2000 SRS allows the Exchange 2000 system to emulate an Exchange 5.5 system (as viewed by the rest of the Exchange 5.5 organization). SRS translates directory information between the Exchange 5.5 DS and Active Directory. SRS incorporates the Exchange 5.5 intra and inter site replication engines to connect to Exchange 5.5 servers and the ADC. It has complete knowledge of the organization topology and adapts itself to any changes, preventing any interruption of service or loss of data.

The SRS is a modified Exchange 5.5 directory on the Exchange 2000 server - allowing replication between SRS (Exchange 2000) and remaining Exchange 5.5 servers as before. It is used as the Exchange 2000 side of the ADC Configuration CA. The SRS allows ITG to avoid reconfiguring the endpoint of a CA every time an Exchange 5.5 server in a site is upgraded to Exchange 2000 during the migration. It also enables the use of Exchange 2000 servers as bridgeheads to legacy Exchange 4.0/5.x sites, through standard mail-based replication (MBR).

The RUS, integrated with the system attendant, operates on a continuous polling basis, determining which objects show in the MAPI address book on GCs, and applies recipient policies (including proxy address). During the polling period, the service searches for all objects matching a set of specified rules. When Exchange 2000 is installed, setup creates an Address List configuration object for that particular domain, and clients querying for address lists notice no difference. ITG also uses RUS to set the proxyAddress for users, as well as other attributes such as the homeMDB, home MTA and/or msExchHomeServerName.

Team Structure

ITG formed its Exchange 2000 deployment project team from multi-faceted technologists who contribute to product research, design, implementation and support. This group is responsible for controlling, coordinating, and synchronizing the delivery of deployment tasks so that project goals and milestones are achieved in a timely fashion. Team experts represent product development, product support and several ITG areas of focus, including:

- Infrastructure and Server Deployment
- Information Security and Accounts Administration
- Messaging
- Data Networking

- Telecommunications
- Management and Tools
- Line of Business Application Compatibility
- Desktop Deployment
- Active Directory Design and Integration (Schema Architect/Administrator)

One of the enterprise benefits of Active Directory is schema extensibility. The schema enforces both the structure and content of Active Directory. Since Active Directory is an enterprise-wide directory service, all changes to the schema have potential enterprise-wide impacts. Schema changes are also permanent, and cannot be reversed. Unmanaged schema extensions could potentially adversely impact the entire network infrastructure. Exchange 2000 is the first Microsoft application extending the schema, and in evaluating potential impacts, ITG realized the need for a central authority for schema (and by implication – content) management.

In the two DS environment, different ITG groups had separate and clear roles/responsibilities. For example, the Exchange *MessageOps* group "owned" the creation and management of mailbox objects. The Windows *Accounts* group owned creation and management of user objects. As the Exchange directory and Active Directory services merged these two objects into one, however, it became clear that someone needed to be responsible for the management of these objects, and, by extension, management of the Active Directory schema that holds them. This overlap of required knowledge revealed a need for a new role in the organization – temporarily called Schema Architect/Schema Administrator (SAA).

The SAA's role is a hybrid – including some of the responsibilities formerly held by Exchange administrators, and others once under Windows administrator control, as well as new responsibilities related to the new integrated directory environment including:

- Development of a schema tracking database and monitoring/management tools to identify who extends the schema, why, and with what information. This allows future groups to locate schema extensions and determine if the information they wish to access (for a new workflow or line of business application, for example) already exists in Active Directory.
- Management of schema extensions, for any reason. The SAA evaluates schema extensions against base schema and proposed extensions.
- Installing the ADC and configuring CAs. For example, the account used to install the ADC must have full administrative permissions to Active Directory (including permissions to modify the schema), as well as Exchange 5.5 and Exchange 2000 full administrator and Account Operator permissions. ITG's pre-Exchange 2000 administrative model separates messaging and Windows 2000 administrator permissions. Exchange administrators had full permissions to Exchange, but not

Active Directory. Windows administrators had user account permissions, but no permissions on mailboxes.

- Management of schema content. For example, deciding the impact of adding directory object attributes to GC replication, because excessive indexing of GC attributes potentially degrades query performance.

The SAA role is indicative of the new level of interoperation and interdependence between the ITG groups managing Windows and Exchange. For example, SAA Exchange 5.5 server roles and permissions are summarized in Table 5.

Exchange 5.5 Right	Service Account Admin	Permission Admin	Admin	View-Only Admin	User	SAA
Add Child	Yes	Yes	Yes	No	No	Yes
Modify User Attributes	Yes	Yes	Yes	No	Yes	Yes
Modify Admin Attributes	Yes	Yes	Yes	No	No	Yes
Delete	Yes	Yes	Yes	No	No	Yes
Send As	Yes	No	No	No	Yes	Yes
Mailbox Owner	Yes	No	No	No	Yes	Yes
Logon Rights	Yes	Yes	Yes	No	Yes	Yes
Replication	Yes	No	No	No	No	Yes
Modify Permissions	Yes	Yes	No	No	No	Yes
Search	No	No	No	No	No	Yes

Table 5: Exchange 5.5 Roles/Permissions

Team Goals

ITG's Exchange 2000 deployment effort integrates goals, objectives and requirements from three distinctly different perspectives:

- **The User Perspective**: Minimize disruption in user service and provide a system offering high business value. Minimize *Client Impact* to 4 to 8 hours per upgrade.
- **The ITG Perspective**: Provide system improvements in performance, availability and reliability. Reduce administration and total cost of ownership. 100% *Worldwide User Deployment* at release to manufacturing (RTM).
- **The Product Development Perspective**: Provide feedback and product testing in a real world environment, to help create a better messaging product. Provide real life *Product Testing & Feedback*.

Timeline

ITG's Exchange 2000 production planning effort was also constrained throughout by the overall development and deployment schedules for both Windows 2000 and Exchange 2000, as shown in Table 6. This deployment strategy is roughly followed for each of the many beta products ITG simultaneously deploys before RTM. Keeping frequent revisions of both the network operating system and Exchange synchronized proved one of ITG's greatest challenges.

The Exchange 2000 deployment team broke the project into three basic phases, which synchronized with ongoing developmental releases of both Windows 2000 and Exchange 2000.

Phase 1: Early Redmond Implementation – A limited deployment on a new Exchange 2000 server using the Beta Exchange 2000 and Windows 2000 RTM code base.

Phase 2: Expanded Early Implementation – A limited rollout to about 4, 000 users in Redmond, Dublin and at least one other remote site using Exchange 2000 release candidate (RC) and Windows 2000 RTM code base.

Phase 3: Global Implementation – Worldwide implementation of Exchange 2000 beginning with the RC code base and continuing into the RTM code release, running on the released version of Windows 2000.

Exchange 2000	Beta	RC1	RC2	RTM
Users	300	4,000	100%	100%
Servers	1 – MSG (Messaging) 1 – IMC 0 – HUB 0 – PFS 0 – FBS 1 – OWA	3 – MSG 4 – IMC 2 – HUB 1 – PFS 1 – FBS 1 – OWA	90% Redmond[5] 100% Dublin 1 SDR (Site Data Room)	100%
Services & Features Deployed	ADC GC Proxy Multi-MDB OWA Server	Clustering NetIQ	KMS[6] RTC[7]	

Table 6: Deployment Timeline

Planning Considerations

Although all supported options are used, for most cases ITG chose the "swing" method from the supported options for Exchange 2000 installation: in-place upgrade, move user, or swing. "Swing" is defined as installing Exchange 2000 on additional hardware as a member server in the appropriate domain, then joining it to an existing Exchange 5.5 site in that domain. Exchange 5.5 mailboxes are moved (using the Move Mailbox function in the Windows 2000 Active Directory Users and Computers MMC snap-in) from an Exchange 5.5 server to the new Exchange 2000 server. Individual users experience a limited amount of downtime (less than 60 minutes per user, depending on mailbox size and network speed) using this method. Another advantage of this method is that Exchange installation can be done remotely. ITG recycles the "old" hardware, if sufficient to run Windows 2000 and Exchange 2000, as the next "new" Exchange 2000 server, and the process is repeated. ITG chose this method for most installations because it reduced the number of new servers needed, and "extra" servers were freed up in the worldwide hardware upgrade process that was simultaneously underway.

In order to maintain the ADC services during these moves, ITG installed the ADC on a dedicated member server. This also increases availability of the service and eases monitoring and management. When the migration period is complete, and the last Exchange 5.5 server is retired, the ADC server will also be retired.

[5] A small number of Exchange 5.5 servers are retained for testing purposes.
[6] KMS – Key Management Service
[7] RTC – Real Time Collaboration features.

Timing

When ITG was scheduling an appropriate date for ADC (and subsequent Exchange 2000 server) deployment, many considerations were taken into account, including synchronization of beta versions of software, conflict with critical business dates, hardware deployments, and network traffic overhead.

The deployment team faced the constant challenge of keeping supported versions of Windows 2000 and Exchange 2000 ADC builds in synch, since both were in near-constant revision. The version of the ADC ITG used was dependent on the schema changes made by certain versions of Windows 2000, so the frequent installations of the two versions had to be coordinated.

An important consideration was scheduling the upgrade for a date that did not conflict with or pose an interruption to critical business dates, for example the close of the financial quarter, or a company meeting.

Coordination with the Windows 2000 deployment team's ongoing Windows NT 4.0 primary domain controller (PDC) and backup domain controller (BDC) software and hardware upgrade schedule was crucial. For example, not all remote sites had yet completed scheduled server hardware upgrades, so ITG forecasted performance impact of ADC deployment. Sample test server configurations and CPU utilization for single Pentium class servers (with 128 Mb of RAM) and dual-Pentium II class servers (with 256 Mb RAM) are detailed in Table 7.

CPU Utilization (approximately every 5 minutes)	Usage
Server running the ADC – Pentium class	8-24%
Server running the ADC – Dual Pentium II class	1-12%
Domain controller – Pentium class	6-66%
Domain controller – Dual Pentium II Pentium class	0-30%
Connecting Exchange 5.5 bridgehead – Pentium class	0-91%
Connecting Exchange 5.5 bridgehead – Dual Pentium II class	20-36%

Table 7: Server CPU Utilization

On its "first pass" the ADC would be replicating each and every object that did not previously exist in Active Directory. All those objects would then need to be replicated to every corpnet DC/GC. Sufficient time for GC replication to remote sites prior to Exchange 2000 server deployment had to be accommodated. After this initial pass, only the changed objects would be replicated. Therefore, the forecast had to take into account the slowest corpnet links to remote sites.

Testing over this slow remote link showed:

- When the two directories are static, only a small amount of data is

passed between all components; however, the majority of this small traffic is between the ADC server and the GC.

- Replication data from the Exchange directory to Active Directory appears to be linear. As a rule of thumb for deployment, ITG predicted a data transfer of 140 KB bind + 14 KB per changed object.

Table 8 details some preliminary testing results for the number of network frames and total traffic sent between the different components.

One-way Test	Exchange 5.5/SRS to ADC
No objects to replicate	16 frames/3 KB
One change in the Exchange Server 5.5 DS	24 frames/8 KB
Two changes in the Exchange Server 5.5 DS	27 frames/10 KB
Three changes in the Exchange Server 5.5 DS	30 frames/12 KB

Table 8: Network Traffic Test Results

With a suitable weekend date selected (to minimize network disruption over the slowest WAN links), and the hardware in place, ITG deployed the ADC into its production environment in February 2000 according to its phased plan outlined in the next section of this paper.

Deployment Phases/Checkpoints

Phase 0: Preparation

Exchange 5.5 DS Preparation. Testing of the Exchange 2000 ADC revealed a number of “anomalous” objects in the Exchange 5.5 DS. For the smoothest migration path these objects had to be cleaned up before the first ADC replication. An anomalous object is defined as an Exchange 5.5 mailbox whose **mailNickname** attribute (Exchange 5.5 “alias”) does not match the **loginID** attribute of the primary Windows security principal (user account) in the same domain associated with it.

Known as “resource mailboxes”, these mailbox objects are usually associated with a “resource” managed by any number of different “persons” over time. In other words, at any given moment the Exchange 5.5 (resource) mailbox object with the **mailNickname** “FOO” may have its primary Windows user attribute set as Windows user **loginID** “BAR”. However, the Windows user “BAR” also has an Exchange 5.5 (personal) mailbox of the name “BAR”, resulting in two Exchange 5.5 DS objects with the same primary Windows security principal. In the Exchange 2000 and Windows 2000 environment, each mailbox may have one and only one primary Windows user account in the same domain associated with it. In the Exchange 5.5 environment this one-to-one association was not strictly enforced. In fact, the Exchange 5.5 mailbox was not required to have any association with a security principal, and it was possible for two or more security principals to own the same Exchange 5.5 mailbox.

Over the years, for various business reasons, ITG had created a number of these resource mailboxes that did not match the new rule for Exchange 2000 mailboxes. For example, conference rooms have mailboxes, but the "owner" of those mailboxes changes frequently. To illustrate; an e-mail (and Exchange 5.5 mailbox) name for conference room one in building Z might be represented as "BldgZConf1" in the Exchange 5.5 global address list with an e-mail address of BldgZconf1@ms.com. This mailbox object "BldgZconf1" might be "owned" or associated with Windows user account "Jack" or "Jill" at different times. Mail sent to the conference room in order to reserve it for a meeting would then be read by the Windows user (Jack or Jill) associated with mailbox "BldgZconf1" at that time. However, both Jack and Jill each have their personal mailboxes as well.

Receptionist mailboxes are another example of this kind of resource mailbox. Since receptionists at Microsoft frequently move assignments from building to building, they have found it convenient to leave the e-mail account associated with the "person at the receptionist desk for this building" behind. This might be a different Windows user at any given time. Information and e-mail that the next receptionist for that particular building might need to know are conveniently managed this way. Building occupants always know how to reach the "person" at the front-desk of their building by email in this way.

If this mismatch is not cleaned up before the first ADC replication, the ADC can become confused, and link the wrong "primary" Windows security principal to the mailbox. In the conference room example, if the ADC were to encounter the conference room mailbox with the primary user Jack (Windows security principal) first, it would link the mailbox "BldgZconf1" to that user account (Jack) as the primary owner. Subsequently, when the ADC attempts to match Jack's Exchange 5.5 mailbox (also named Jack) to the user object (Jack), it finds that the user object (Jack) is already linked to the Exchange 5.5 mailbox object BldgZconf1. In that case, Jack is unable to access his personal mailbox, because he is not listed as the "primary" for that mailbox (he is listed as primary for the BldgZconf1 mailbox, and there must be a one-to-one correspondence). In addition, queries to the Global Address List for Jack's address and other information will show the address, phone, and other information of the conference room as Jack's.

The same "resource mailbox" functionality can be achieved in the Windows 2000/Exchange 2000 environment by creating disabled security principals (with no logon rights for security reasons) in Active Directory linked to each resource mailbox. A number of different Windows security principals at different times can then be added as secondary, or alternate, users of that account's mailbox, using the Advanced View tab of the Users and Computers MMC snap-in. Cleaning up the Exchange 5.5 DS in this way before first ADC replication provides the smoothest migration path.

Development Preparation. ITG met with Exchange ADC developers to review the deployment plan and confirm the support plan and escalation procedure.

Server and Systems Preparation. Messaging Engineering, Infrastructure

Engineering and Server Management and Support teams deployed two new servers capable of supporting Windows 2000 and Exchange 2000 ADC. Each was brought online as member servers in the corpnet Windows 2000 domain in two different rooms of the Redmond Corporate Data Center (a standard Data Center procedure to isolate problems with a possible power-outage – each room has a separate power source). One acts as the main system, fulfilling the daily functional requirements of the ADC, while the other acts as a backup, providing redundant functionality in the event of a system failure within the main system. In the event of failure, the backup system would be brought online as soon as the primary system was determined to be down, maintaining ADC functionality until the primary system could either be repaired or rebuilt to act as the backup to the current system. The Windows 2000 member server ITG used for the ADC was sized aggressively, and built with two Pentium II Xeon 450Mhz processors, 256Mb of RAM, 8 Gb hard drive (RAID1) for system files, and 8 Gb hard drive (RAID5) for the ADC.

Accounts Group Preparation. The accounts management group froze changes to the Exchange 5.5 DS over the deployment weekend, and provided communications to the Accounts Group owners.

Operations & Service Management Preparation. Redmond Data Center technicians prepared for intensive monitoring of the ADC service the first twelve hours after ADC deployment, including DC/GC utilization (some details on monitoring are given in the next section of this paper “Phase 4”).

Helpdesk Preparation. The Helpdesk provided a central point of contact for support issues. Helpdesk technicians were prepared to target the source of any possible problems (either the Exchange 5.5 DS or Active Directory) by asking users who might experience difficulty accessing directory information whether they are looking at Active Directory or Exchange DS.

Contingency Plan Preparation. In the event of a problem due to the ADC, ITG prepared the following options to get back to a known working state:

- Turn off the CA.
- If this does not fix the problem, then shut down the ADC service.
- In case of corrupted data, remove the organizational unit where the data was stored, and perform an authoritative restore from tape of a known good state.
- As a last resort, ITG could use a Windows 2000 tool called LDP to hand edit data in Active Directory.

Exchange Organization Preparation. Several steps must be achieved before running Exchange 2000 setup to prepare Active Directory for the mixed environment during migration. These include extending Active Directory schema with schema and display specifiers, group creation and delegation of authority, as well as delegating certain domain level permission to specific Exchange 2000 processes, such as the Recipient Update Service. Explicit Access Control List (ACL) modifications that prevent current domain and Enterprise Admins from obtaining Exchange 2000 admin permissions due to inheritance must also be performed, so that during the

migration the old administrative structure is preserved. In order to accomplish this in an environment where Active Directory admins, Exchange 5.5 admins, and Windows domain admins all have different permissions, ITG used a set of Exchange 2000 setup command–line switches known as OrgPrep. OrgPrep comprises two setup command-line switches, ForestPrep and DomainPrep:

- SETUP /ForestPrep - is run in the root domain and performs tasks such as extending the Active Directory schema, creating the Exchange 2000 Servers groups, creating the Exchange 2000 Organization object in the configuration naming context, and setting up the permissions structures. The account used to run this switch must be logged on with Enterprise Admin, Domain Admin, Schema Admin, and Local Admin (to write to the log file) privileges. In addition, in order to join the existing Exchange 5.5 organization, the account used for installation must have (at least) view only permissions to the Exchange 5.5 directory. During ForestPrep the first full Exchange 2000 Admin account is nominated. This account is used in DomainPrep and to assign delegated Exchange admin rights to other new and existing Exchange admin accounts using the Delegation Wizard. Once this account has been added to the local machine Administrators group it can install the first instance of Exchange 2000 (without having to be an Enterprise, Schema, or Domain Admin). By using the Delegation Wizard, this account can also delegate other users or groups various Exchange 2000 Admin roles. ForestPrep needs to be run only once per organization.
- **SETUP /DomainPrep** - is run after running ForestPrep and after waiting for replication to occur in every domain where an Exchange 2000 server is going to be installed. DomainPrep can be run from any machine in that domain. DomainPrep performs tasks such as creating the necessary global groups for Exchange 2000 administration and Exchange 2000 service access into Active Directory. The account used to run this switch must have Domain Admin permissions into the domain in which Exchange 2000 will be installed. In addition, the account used for this switch must have Exchange 2000 admin permissions (such as the account nominated during ForestPrep).
- ForestPrep and DomainPrep do NOT have to be run if the Windows account installing the first Exchange 2000 server has Enterprise and Schema Admin permissions AND the first install is in the domain that contains the Schema Master.

Phase 1: ADC Installation

For its first installation in the corpnet forest ITG installed the ADC on a Windows 2000 member server meeting or exceeding the minimum requirements for an Exchange 2000 server:

- Intel Pentium 300 megahertz (MHz) or faster processor.
- 128 megabytes (MB) of RAM (256 MB recommended).

- Microsoft Windows 2000 Server operating system.
- At least 2 gigabytes (GB) of available disk space for Exchange 2000 on the installation drive (if installing on top of Exchange 2000).
- At least 500 MB of available disk space on the system drive.
- Page file set to a minimum of twice the amount of system RAM (recommended).
- VGA or higher resolution monitor.
- A CD-ROM drive.
- The Windows account used for ADC installation is not an Exchange 5.5 service account.
- The Windows account used for installation is logged in to the same domain as the server.
- The Windows account used for installation has access to the Global Catalog (must be a member of the Schema Administrators Security Group).
- The Windows account used for installation has Exchange Enterprise Admin rights on the member server giving full access to the registry, counters, Exchange Configuration container and administrative shares (including “Act as part of the Operating System”, “Log On as a Service”, and “Backup/Restore Files and Directories” permissions).
- The Windows account used for installation has Domain Administrator rights for each domain the ADC will connect to (member of the Domain Administrators security group) and for the member server on which the ADC is installed.
- The Windows account used to install the ADC has Exchange 5.5 Server Operator permissions.
- The Exchange 2000 service account specified during setup is a member of the Enterprise Administrators or root Domain Administrators security group (to successfully update user information in all necessary domains).
- Windows 2000 and DNS services are deployed according to the Windows 2000 documentation. Proper implementation of DNS or dynamic DNS services in the Windows 2000 environment is critical to ADC (and Exchange 2000) function.
- The Exchange 5.5 server that is the “target” of the ADC has Exchange Server 5.5 Service Pack 3 or later installed.

Note that ITG routinely segregates servers into dedicated service roles for manageability and reliability. Other services (such as SMTP) co-located on the same server with the ADC present additional configuration complexity.

Phase 2: Object Matching Rules

ADC uses the target container set on the CA to replicate directory objects

that cannot *automatically* be mapped between the two directories. Configurable options for mapping objects include:

- Mailbox-enable an existing Windows 2000 user account.
- Mail-enable an existing Windows 2000 user account.
- Create a Contact in the Windows 2000 container (mail-enabled or mail disabled).
- Do not create any object.

By default, the ADC uses its own rule (located in the configuration container called “Default ADC Policy”) for matching attributes between the two directories. For example, the *department* field in the Exchange directory is automatically mapped to the *department* field in Active Directory.

Matching rules reside in the Default ADC Policy object for the ADC (not CA-specific) in a field called msExchServerXSchemaMap, where *X* equals 1 for Active Directory-to-Exchange mapping and 2 for Exchange-to-Active Directory mapping. Controlling which attributes are replicated can be accomplished using a tool, such as LDP, in binary mode, or through the ADC MMC snap-in. ITG most often accomplishes this kind of task, such as matching the Exchange 5.5 alias name to the Active Directory user name, with scriptable tools, such as LDP.

ITG configured the Exchange 5.5 containers and objects to map and synchronize to their Active Directory equivalents according to the following table:

Exchange 5.5 DS object	Active Directory Object
An Exchange 5.5 **Mailbox** object mapped to an Active Directory account appears in the Exchange directory as a **Mailbox** object. The **Object-GUID** attribute of the Exchange **Mailbox** object is set to the **GUID** of the Active Directory object. All directory attributes from the two objects, such as telephone number, postal address, and so on, are merged and populated to both directory objects.	Maps to Active Directory as a **mailbox-enabled User** (the **msExchHomeServerName** attribute is set to the existing Exchange 5.5 mailbox). The **legacyExchangeDN** attribute of the Active Directory object is set to the Distinguished Name (**DN**) of the matching object in the Exchange 5.5 DS. All directory attributes from the two objects, such as telephone number, postal address, and so on, are merged and populated to both directory objects.
A Distribution List in the Exchange 5.5 directory appears in Active Directory as a **mail-enabled Group** object (type: **Distribution**, scope: **Universal,** or **UDG**).	Because the **DL** object may appear in Active Directory before the membership objects exist, any orphaned members are binary encoded and written to the **unmergedAtts** attribute in the corresponding entry of the **Group** object. This ensures that

	membership changes to the Active Directory **Group** object successfully replicate back to the Exchange directory when two-way CAs are used. The unmerged attributes are only removed and resolved after a full replication of the object is initiated.
A **Custom Recipient** (of any address type) in the Exchange 5.5 directory.	Appears as a **mail-enabled Contact** in Active Directory.

For simplicity, and to retain the same container structure in the Active Directory service, ITG created a single CA for each domain, consolidating all Exchange containers into a single “ADC managed” ou in Active Directory. Once the objects have been replicated, Windows administrators use the Active Directory Users and Computers MMC snap-in to move those objects to the correct ou. The ADC retains the relationship between the two objects through the object-GUID match even though they have been moved.

Figure 3 shows the Default ADC property pages for the MMC snap-in used to define the attributes to replicate between the two directories, and what the matching rules are.

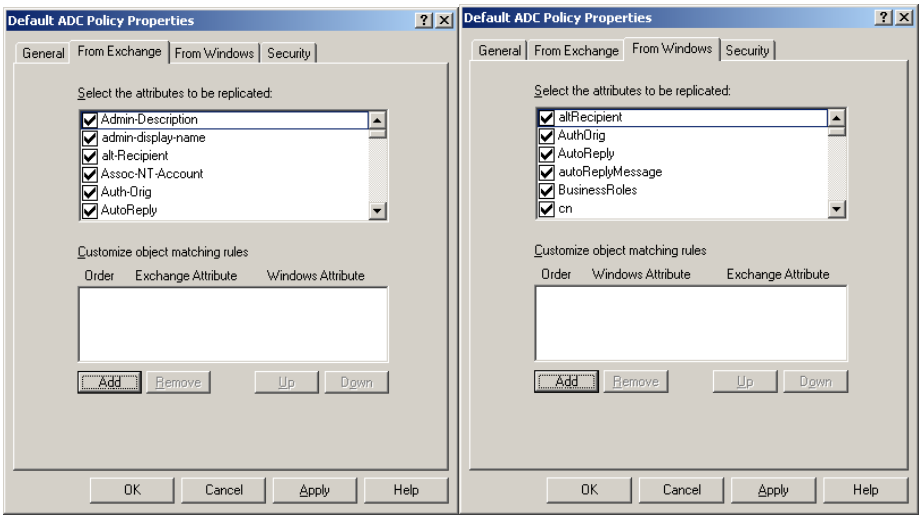

Figure 3: Property Mapping

Phase 3: CA Configuration

The ADC creates two kinds of configuration agreements, configuration CAs (automatically created) and “user” CAs (manually created by the Administrator).

Configuration CAs are configured automatically by an Exchange 2000 server rather than ITG having to instantiate them manually. Additionally, the agreement for replicating configuration context data is between Active

Directory and the SRS rather than Active Directory and each Exchange 5.5 server.

The first Configuration CA created by the SRS has the name of Master_Config CA_*ORGNAM.* Although this can be seen in the ADC MMC snap-in, the agreement is read-only, and thus cannot be modified. After replication, all Exchange 5.5 sites are represented in Active Directory as administrative groups (AG), and conversely, Exchange 2000 servers in AGs are represented in Exchange 5.5 as sites, allowing ITG to manage these objects from either “side” of the CA.

Configuration CAs have a number of properties ITG can manipulate, including:

- **MsExchReplicateNow.** A Boolean value. If **True**, the ADC performs a replication cycle immediately for the CA. This flag is usually set by the ADC Administration MMC snap-in in Windows 2000. Because it exists within the Configuration naming context that is replicated around the forest, it can be set remotely.
- **msExchServer1HighestUSN.** This is the highest update sequence number last found in Active Directory.
- **msExchServer2HighestUSN.** This is the highest update sequence number last found in the Exchange 5.5 directory.
- **MsExchDoFullReplication.** A Boolean value. If **True**, the two directories are refreshed.
- ***USNChanged.*** The USN assigned to the CA object at last update.

ITG created one user CA for each Windows 2000 domain, as illustrated in Figure 5. Each CA targeted one Exchange 5.5 server in the site for that domain as a “bridgehead” server for that site. Initially, ITG deployed these CAs as one-way only, from the Exchange 5.5 DS to Active Directory, so that replication traffic could be easily monitored, and object/attribute fidelity could be verified.

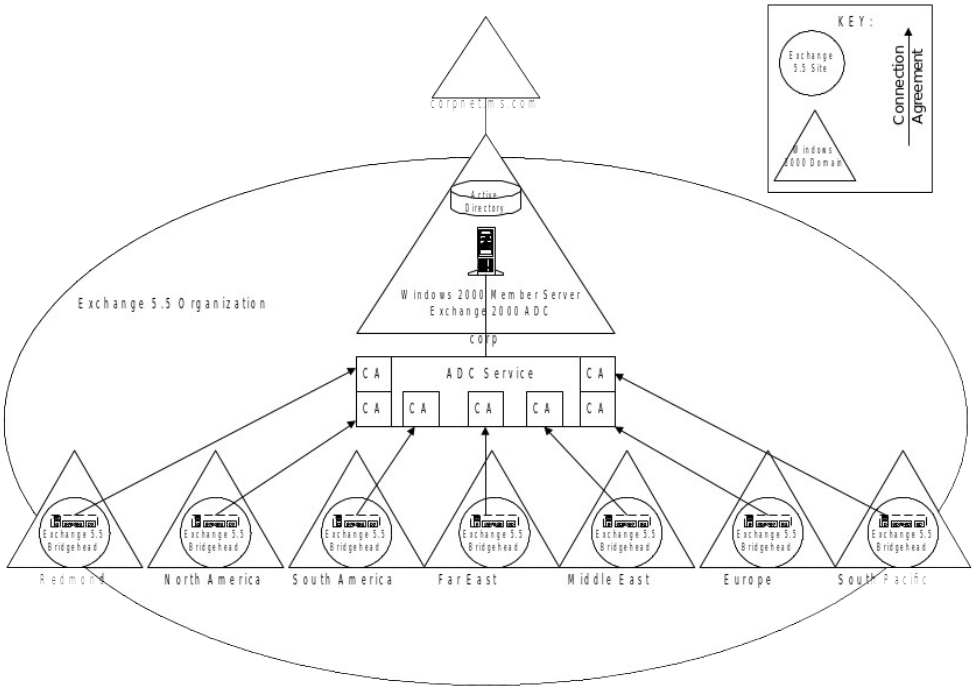

Figure 5: CA Deployment

Phase 4: Monitoring

ITG uses a variety of internally developed and third party tools to monitor and report on server and service operations**.** At the time of this writing, which tools will be released in the Exchange 2000 Resource Kit has not yet been finalized.

- **WebMon:** This internally developed tool (using Windows Management Instrumentation) provides ITG troubleshooters a simple Web interface for viewing Exchange 2000 server status. WebMon returns information such as link status, CPU utilization, disk space, memory utilization, queue lengths and service status.
- **ADCDiag:** is used to find duplicate **LegacyExchangeDN** attribute values in Active Directory.
- **LDAPMOD:** is a command-line LDAP modifier.
- **Event Logs**

The ADC logs several categories of events to the application event log, as shown in Table 9.

Category	Description
Replication	Shows messages indicating events that occurred during replication.
Account Management	Shows messages indicating events that occurred while attempting to write or delete an object during replication.
Attribute Mapping	Shows messages indicating events that occurred while mapping attributes between Active Directory and Exchange directory.
Service Controller	Shows events that occurred while the service is started or stopped.
LDAP Operations	Shows events that occurred while accessing the directory using LDAP.

Table 9: Application Event Log Categories

Since the log files are not deleted by default, ITG leaves the (default) logging level set to “None” unless actively troubleshooting an issue. Table 10 summarizes the most important ADC application EventIDs monitored and remedial actions taken in response.

Event ID	Description	Explanation	Action
8084	Could not load mapping table.	Active Directory Connector could not load mapping table.	Verify that the ADC account has permission to read the Connection Agreements and all of their attributes.
8113	The service could not be initialized because the necessary file X could not be found. Make sure that the operating system was installed properly.	Active Directory Connector service initialization failure: missing file.	Check the file version and verify that its location is in executable path.
8114	The service could not be initialized because the necessary entry point X could not be found in the file Y. Make sure that the operating system was installed properly.	Active Directory Connector service initialization failure: entry point could not be found.	Check the file version and verify that its location is in executable path.
8026	Connection is down.	The DC with the connection agreement is down.	

Event ID	Description	Explanation	Action
8142	Active Directory Connector unexpected exception.		Restart the service. Verify that there is enough disk space and memory.
8143	Active Directory Connector out of memory exception.	Out of Memory exception.	Increase the swap file size, close some other applications, or restart the service.
8144	Exception X was raised at address Y.	Active Directory Connector exception.	Restart the service. Verify that there is enough disk space and memory.
8002	The service was stopped.	Active Directory Connector service stopped.	The Service Control Manager has returned this request. The service was shutdown successfully. This message requires no action and is informational only.

Table 10: ADC Application EventID

Performance Monitor

The counters “of interest” for Exchange 2000 servers are very similar to those monitored for an Exchange 5.5 server, as summarized in Table 11. ITG generally logs these to disk for later review, unless needed for active troubleshooting. Perfmon.exe logs are viewed in Exchange 2000 through the System Monitor MMC snap-in.

Object	Counter	Instance	Color	Scale
Processor	% Processor Time	1 – n	Red, [Black, Dk Blue, Dk Green]	1
Process	% Processor Time	EMSMTA	Blue	1
Process	% Processor	MAD	Pink	1

	Time			
Process	% Processor Time	Store	Yellow	1
Process	% Processor Time	INETINFO	Green	1

Table 11: PerfMon Counters

In addition, ITG uses a third-party tool called AppManager from NetIQ for a variety of monitoring and general health reporting functions across Exchange 2000 servers, including the following:

NetIQ Monitoring

- **MSExchangeIS service stopped** on all servers.
- **IISADMIN service is stopped** on Instant Messaging servers.
- **SMTP service is stopped** on Internet Mail Connector servers.
- **Logical disk space available low** on all servers. Monitors available disk space on the Information Store drives and the Log Files drives to ensure that available space does not drop below 20% or 1GB.
- **Number of messages in IMC/MTA queues**.
- **Date of most recent successful backup**.

NetIQ Reporting

Historical data regarding the number and length of outages to report an uptime percentage for the month are gathered for the following:

- **Information Store availability.**
- **SMTP availability.**
- **Instant Messaging availability.** Delivery of messages via the Instant Messaging service is interrupted when the IISADMIN service is stopped on one of the servers.
- **Message Response Time.** Messaging Operations tracks the average delivery times from Redmond to different sites around the world, sending test messages once per hour during normal business hours to collect response time data.
- **Messages through SMTP.** In order to determine the volume of mail that passes between Microsoft and the Internet, ITG uses AppManager to count the number of messages that are sent and received each day.
- **Messages received on mailbox servers**. To determine volume of messages that are transferred through the messaging system internally, ITG tracks the number of messages received on each of the message servers.
- **Information Store growth.** Gives ITG an indicator of how to optimize server sizes and user distribution.

Exchange 2000 deployment planning was complicated by the near

simultaneous deployment of a new network operating system and infrastructure. Additional focus and unprecedented inter-group cooperation was key to success. The first lesson ITG learned was that early planning is extremely important to a successful deployment with minimum user disruption. This is especially true in the Windows 2000 and Exchange 2000 environment. Additional lessons ITG learned include:

- Understand the differences between an Exchange 5.5 mailbox object and a Windows 2000 mailbox-enabled object clearly. Ensuring that the Exchange 5.5 DS is “Exchange 2000 ready” **before** ADC installation will help ensure a smooth migration. This means that there should be a one-to-one correspondence between the Exchange 5.5 object and Active Directory security principal.
- Create ADC connection agreements between a GC and Exchange Server, or deploy the ADC in close network proximity to a GC. Because the ADC never “finishes” during the migration (its purpose is to keep the two directories synchronized), for best performance, ease of management and increased availability, install ADC on a dedicated Windows 2000 member server.
- Place the server hosting ADC on the same subnet as the Exchange 5.5 directory and Active Directory bridgeheads, if possible.
- Use Directory Replication Bridgehead servers to facilitate Exchange 5.5 server directory replication between Exchange Server sites. Where possible, use them as ADC bridgehead servers for connection agreements. These servers should be the last servers migrated to Exchange 2000 for simplicity.
- Clearly understand the differences in the directions of connection agreements. For example, the results of two “one way” agreements may be different than the results of one “two way” CA. Care should be taken when configuring the “From Windows” and “From Exchange” tabs of the CA MMC snap in, as well as the source and target containers. In order to obtain the desired results, match both the correct containers and the direction of information flow.
- Allow sufficient time after OrgPrep (ForestPrep and DomainPrep) and ADC installation for complete replication around the environment. Initially, object replication may take some time, especially in larger environments, as all objects are “new” the first time. After the first peak of replication traffic, only ongoing incremental changes are replicated, until the last Exchange 5.5 server is retired from the environment
- Synchronize the entire Exchange 5.5 site instead of synchronizing individual recipient containers. Choosing the entire Exchange 5.5 site as the source and target of the CA on the Exchange Server, and also choosing the Active Directory domain as the source and target on the Active Directory side of a two-way CA effectively synchronizes the Exchange 5.5 recipient container hierarchy with the ou hierarchy in Windows 2000. The ou hierarchy or the location of individual recipients created in Active Directory by the ADC can be changed at a later time.

- Understand security implications of groups clearly. Access control and group usage require careful planning. Because Active Directory groups are used for both access control and distribution lists, careful planning is required to prevent modifications to group membership (when the ADC maps Exchange 5.5 DLs to Active Directory groups) that adversely impact system security.
- Cross department coordination is essential. ITG, the product development team, client support, PSS and the users themselves, all participated and cooperated in the rollout of Exchange 2000. This was essential because all groups were working with new products. Members of each department, from development, through ITG, to PSS, had to become familiar with the latest features in both Exchange 2000 and Windows 2000.

ITG’s initial plans for design and deployment of the Exchange 2000 Active Directory Connector service at Microsoft were intimately connected with the overall deployment plans for Windows 2000 and Exchange 2000. Although deploying Microsoft products into production while in beta code can sometimes be at odds with the goal of running the IT utility, the combination of Windows 2000 server on the backend and Windows 2000 Professional on the desktop has already yielded bottom-line benefits to Microsoft by simplifying and centralizing network administration and consolidating server hardware.

Future Steps

In addition, the ITG deployment of the Exchange 2000 Active Directory Connector set the stage for full deployment of Exchange 2000, giving Microsoft employees a rich set of new features, including:

- A larger user mailbox (because of Exchange 2000 support of multiple storage groups).
- Integrated videoconferencing.
- Wireless smartphone connectivity.
- Access to Exchange 2000 mailbox information from virtually anywhere, anytime, from any device.

Conclusion

In the early stages of Exchange 2000 production deployment ITG encountered both challenges and opportunities in the corpnet environment that had to be addressed. ITG is sharing these "lessons learned" in hopes that, when applicable, customers can benefit from ITG’s experiences. The volume of messaging traffic, the integral role of users in product development and testing, and high user sophistication and support expectations make Microsoft a unique environment for Exchange 2000. However, all these factors were managed successfully with communication, planning, testing and cooperation. As Microsoft continues to deploy Exchange 2000, Windows 2000 Server and Windows 2000 Professional, ITG will continue to share its experiences with customers.

FOR FURTHER INFORMATION

To view additional IT Showcase material please visit
http://www.microsoft.com/technet/showcase

Deploying the Active Directory Connector Whitepaper
http://www.microsoft.com/TechNet/exchange/technote/actdir2k.asp

Windows 2000 Server Deployment Planning Guide: Chapter 20 – Synchronizing Active Directory with Exchange Server Directory Service

http://www.microsoft.com/TechNet/win2000/dguide/chapt-20.asp#d

Microsoft Exchange Server 5.5 Advanced Backbone Design and Optimization Whitepaper
http://technet.microsoft.com/cdonline/content/complete/srvnetwk/exch/technote/backtraf.htm

Design Considerations for Windows 2000 Active Directory with Exchange 2000 Server in Mind Whitepaper
http://www.microsoft.com/exchange/prodinfo/2000/ADIntegration.doc

XADM: Installing the ADC on a Windows 2000 Domain Controller That Also Runs Exchange Server

http://support.microsoft.com/support/kb/articles/Q250/9/89.ASP

For any questions, comments, or suggestions on this document, or to obtain additional information about Microsoft IT Showcase, please send email to showcase@microsoft.com